UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/083,010	02/26/2002	Matthew Charles Priestley	MS190438.1	4314

27195 7590 06/16/2008

AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
06/16/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
lpasterchek@thepatentattorneys.com

Office Action Summary	Application No.	Applicant(s)	
	10/083,010	PRIESTLEY ET AL.	
	Examiner	Art Unit	
	SHANTO M Z ABEDIN	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-18,20-27,31 and 32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-18,20-27,31 and 32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/02/2008 has been entered.

2. Claims 1, 3-18, 20-29, 31 and 32 are pending in the application.

3. Claims 1, 3-18, 20-29, 31 and 32 are rejected.

Response to Arguments

4. The applicant's arguments regarding the previous 35 USC 101 type rejections are fully considered. The previous 35 USC 101 type rejections of claims 1, 3-16 and 28-29 are withdrawn because of the amendments made to the claims. 35 USC 101 type rejections of claims 31-32 are maintained (please see the explanation below)

5. The applicant's arguments regarding the 35 USC 103 (a) type rejections of claims 1 and 3-17 are fully considered, however, found not persuasive. In particular, the combination of the cited references does teach the limitations set forth by the newly amended claims (please see below for detail explanation)

6. The applicant's arguments regarding the 35 USC 103(a) type rejections of claims 18, 20-27 and 31-32 are fully considered, however, moot in view of new grounds of rejection presented in this office action.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 27 and 31-32 are rejected under 35 USC 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claim 27, it is directed to a computer executable system comprising means plus functions. However, claim languages fail to disclose any associated machine, or computer hardware. Firstly, a "computer executable system" recited in the preamble implicitly disclosing a system of/ comprising computer executable codes or programs. Secondly, according to the specification (Fig 1, and Page 14, lines 7-16; the invention has been described above in the general context of computer-readable instructions of a computer program.....invention also may be implemented in combination with other program modules) all of the claimed 'means' can be implemented in software alone. Therefore, claimed invention is considered to be non-statutory as being directed to non-statutory functional materials. See MPEP 2106.01

Regarding claims 31-32, they are directed to a system. However, actual claim limitations fail to disclose any associated machine or computer hardware - computer memory and processor are recited only in preambles of the claims. Furthermore, according to specification all of the claimed features such as a service, a wrapper, and a pass-phrase could be implemented in software alone (please see specification, Fig 1, and Page 14, lines 7-16; the invention has been described above in the general context of computer-readable instructions of a computer program.....invention also may be implemented in combination with other program modules.) Therefore, claimed invention is

considered to be non-statutory as being directed to software/ program implemented components. See MPEP 2106.01

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 1, 3-17 and 31-32 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claims 1, 3-17 and 31-32 they recite " ..the following components executable by processor: a wrapper that packages credentials associated with resources of a service; and a pass-phrase employed in connection with generation of cryptographic wrapping key..", or "the following components stored in a computer memory and executable by a processor: a service…a wrapper generated by the service… and a pass-phrase employed to generate the wrapper..". Therefore, according to the claim limitations feature/ component such as a 'pass-phrase' is computer executable.

However, according to the specifications, executables are different from a 'pass-phrase'. In particular, according to the specification (please see Page 12, line 21- Page 13, line 29) a wrapped credential and/ or password is stored in an executable file or package or wrapper. Therefore, while the storage of the pass-phrase can be executable, **a pass-phrase itself can not be interpreted as an**

executable component, and consequently, the claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 6-15, 17, 27 and 31-32 are rejected under 35 USC 103 (a) as being unpatentable over Brainard (SecurSight: An Architecture for Secure Information) in view of Hypponen (US 6986050 B2) further in view of Bathrick et al (US 5825300).

Regarding claim 1, Brainard discloses a system that facilitates processing credentials, comprising:

a computer memory having stored thereon (Page 3-4; Section 2 and 2.2; credential storage in desktop or smartcard) the following components executable by a processor:

a wrapper that packages credentials associated with resources of a service (Page 2, Section 1.2 to Page 4, Section 2.2; Page 6, Section 3.5; a wrapper for secure credential communication; encrypted or locked or protected PSD, or PAC/ EAR including keys/password/ certificate also interpreted as wrapper) ; and

the wrapping key is utilized to generate a wrapper that encapsulates the credentials (Page 3-4 and 6, section 2.2, 2.3 and 3.5; an encryption key derived from password, or a KEK, or a PUK, or

(unlocking) key is utilized to create an encrypted/ wrapped/ locked PSD or PAC that encapsulates authentication credentials/ keys/ password), and

the credentials employed to provide encrypted communication between a user and the service that facilitates access to the resources of the service (Page 2, Section 1.2 to Page 4 Section 2.2; credentials such as a key or KEK or PUK or password employed to create wrappers/ locked PSD / encrypted PAC to provide encrypted/ secure communication in the application- based services in network; also see SSL communication).

Brainard discloses the system wherein a password, or key is used to generate a cryptographic wrapping key, or protect other credentials. However, Brainard fails to disclose use of a pass-phrase for that purpose, in particular, Brainard fails to disclose expressly:

a pass-phrase employed in connection with generation of a cryptographic wrapping key, the pass-phrase employed to facilitate access to the credentials, and

the pass-phrase distributed separately from the credentials.

However, Hypponen discloses a pass-phrase employed in connection with generation of a cryptographic wrapping key (Col 3, lines 35-65; generating cryptographic key from passphrase), the pass-phrase employed to facilitate access to the credentials (Col 3, lines 15-25; passphrase is employed to encrypt/decrypt password/ credential in case of password based symmetric cryptographic key).

Modified Hypponen-Brainard system fails to disclose the pass-phrase distributed separately from the credentials.

However, Bathrick et al discloses the pass phrase distributed separately from the credentials (Col 2, lines 33-40, 64-67; Claim 1; distributing keying and certificate material separately; the examiner interprets keying material as pass-phrase, and certificate material as credential).

Furthermore, at the time of invention, it would be logically obvious (from the teachings of modified Hypponen-Brainard system) to a person of ordinary skill in art to design a system wherein a pass-phrase is utilized (instead of a password) to generate a cryptographic wrapping key, and facilitate access to the credentials.

Hypponen, Bathrick et al and Brainard are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Hypponen with Brainard for employing pass-phrase in connection with generation of the wrapper via a cryptographic wrapping key in order to provide a pass-phase based protection, and to combine teachings of Bathrick et al with modified Hypponen -Brainard system to provide further protection against unauthorized access to the passphrase and the credential.

Regarding claim 6, Brainard discloses the system of claim 1, further comprising one or more partners to request access to the resources (Section 1.2, 3.3; agents, application servers/ authentication services)

Regarding claim 7, Brainard discloses the system of claim 6, at least one of the partners includes a credential store to manage the credentials (Section 2.2; manager, or authentication server or application server or issuer for generating and storing credentials).

Regarding claims 8 and 9, these limitations are already addressed in terms of rejecting claims 1, 6-7. Therefore, they are rejected applying as above rejecting claims 1 and 6-7.

Regarding claims 10-12, Brainard discloses use of that pass phrase over a SSL connection or in a VPN environment (Page 6, Col 1, step 5, application server, SSL connection); and issuing an Electronic License Certificate (Section 3.1; PAC or PSD containing certificate).

Regarding claims 13-14, Brainard teaches a platform provisioning service, or such service (Page 2; Page 5, Fig 5, SecurSight authentication service; application based services on network, and authentication services are interprettted as provisioning services) being associated with a partner including a service provider and tenant (Page 2; Page 5, Fig 5; system consist of manager, desktop, and application server; Brainard's enterprise network resources and applications imply capability of performing billing, financial, or accounting functions)

Regarding claims 15 and 17, these limitations are already addressed in terms of rejecting claims 1, 6-7 and 13-14, therefore, they are rejected applying as above rejecting claims 1, 6-7 and 13-14.

Regarding claim 27, it is rejected applying as same motivation as applied above rejecting claim 1, furthermore, Brainard discloses a computer executable system to facilitate a security relationship between parties, comprising:

means for generating credentials comprising at least a password (Page 3- 6; credential generator, or issuer for generating and distributing credential/ PSD/ PAC including password);

means for generating a package of credentials by wrapping the credentials with a cryptographic wrapping key, wherein the credentials are encapsulated by the wrapper (Page 2, Section 1.2 to Page 4 Section 2.2; Page 6, Section 3.5; manager, or server, or credential issuer for generating wrapper, or encrypted PSD, PAC/ EAR; PAC or PSD containing encrypted passwords/ keys/ certificate; locking/ wrapping credential with KEK, or unlocking key)

Brainard fails to disclose

means for generating a pass-phrase; and cryptographic wrapping key derived from the pass-phrase; means for transmitting the package and the pass-phrase to a system via different communications mediums; and means for storing the credentials separate from the pass-phrase.

However, Hypponen discloses means for generating a pass-phrase; and cryptographic wrapping key derived from the pass-phrase (Col 3, lines 35-65; generating cryptographic key from passphrase), the pass-phrase employed to facilitate access to the credentials (Col 3, lines 15-25; passphrase is employed to encrypt/decrypt password/ credential in case of password based symmetric cryptographic key).

Modified Hypponen-Brainard system fails to disclose means for transmitting the package and the pass-phrase to a system via different communications mediums; and means for storing the credentials separate from the pass-phrase.

However, Bathrick et al discloses means for transmitting the package and the pass-phrase to a system via different communications mediums; and means for storing the credentials separate from the pass-phrase (Col 2, lines 33-40, 64-67; Claim 1; storing, and distributing keying and certificate

material separately; the examiner interprets keying material as pass-phrase, and certificate material as credential).

Furthermore, at the time of invention, it would be logically obvious (from the teachings of modified Hypponen-Brainard system) to a person of ordinary skill in art to design a system wherein a pass-phrase is utilized (instead of a password) to generate a cryptographic wrapping key, and facilitate access to the credentials.

Regarding claim 31, it is rejected applying as same motivation as applied above rejecting claim 1, furthermore, Brainard discloses a system to establish a trust relationship, comprising the following components stored in computer memory and executable by a processor:

a service that controls one or more resources, the service issues credentials to facilitate access to the resources (Page 2 and 5; manager, or application server for managing services on network; granting services after authenticating credentials/ PSD);

a wrapper generated by the service to package the credentials, the credentials encapsulated in the wrapper (Page 2, Section 1.2 to Page 4 Section 2.2; Page 6, Section 3.5; manager, or server, or credential issuer for generating wrapper, or encrypted PSD, PAC/ EAR; PAC or PSD containing encrypted passwords/ keys/ certificate; locking/ wrapping credential with KEK, or unlocking key)

Brainard fails to disclose a pass-phrase employed to generate the wrapper and mediate access to the service, the pass-phrase distributed separately from the credentials.

However, Hypponen discloses means for generating a pass-phrase; and cryptographic wrapping key derived from the pass-phrase (Col 3, lines 35-65; generating cryptographic key from

passphrase), the pass-phrase employed to facilitate access to the credentials (Col 3, lines 15-25; passphrase is employed to encrypt/decrypt password/ credential in case of password based symmetric cryptographic key).

Modified Hypponen-Brainard system fails to disclose means for transmitting the package and the pass-phrase to a system via different communications mediums; and means for storing the credentials separate from the pass-phrase.

However, Bathrick et al discloses means for transmitting the package and the pass-phrase to a system via different communications mediums; and means for storing the credentials separate from the pass-phrase (Col 2, lines 33-40, 64-67; Claim 1; storing, and distributing keying and certificate material separately; the examiner interprets keying material as pass-phrase, and certificate material as credential).

Furthermore, at the time of invention, it would be logically obvious (from the teachings of modified Hypponen-Brainard system) to a person of ordinary skill in art to design a system wherein a pass-phrase is utilized (instead of a password) to generate a cryptographic wrapping key, and facilitate access to the credentials.

Regarding claim 32, Brainard discloses the system the service is a provisioning service that establishes a trust relationship between one or more partners *via* the credentials (Page 2; Page 5, Fig 5, SecurSight authentication service; application based services on network, and authentication services are interprettted as provisioning services; accessing services upon authenticating credentials or PSD).

10. Claim 16 is rejected under 35 USC 103 (a) as being unpatentable over Brainard (SecurSight: An Architecture for Secure Information) in view of Hypponen (US 6986050 B2) further in view of Bathrick et al (US 5825300) further in view of Kay et al (US 6993555B2).

Regarding claim 16, Kay et al discloses at least one of the platform provisioning service and the partner maintain an account to process the credentials, **the at least one of** the platform provisioning service and the partner employ a Universal Resource Locator (URL) to present the credentials to the account (Col 11, starts at line 64; URL containing authentication information).

Kay et al and Brainard are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Kay et al with modified Brainard method to design a method employing a Universal Resource Locator (URL) to present the credentials to the account in order to provide an access request with the access credentials.

11. Claims 3-5 are rejected under 35 USC 103 (a) as being unpatentable over Brainard (SecurSight: An Architecture for Secure Information) in view of Hypponen (US 6986050 B2) further in view of Bathrick et al (US 5825300) further in view of Rahman et al (US 7114080 B2).

Regarding claim 3, Rahman et al discloses the credentials providing stronger encryption than the pass-phrase (Col 3, starts at line 4; Col 7, starts at line 50; using strong password; the examiner interprets such strong password usually has stronger encryption than an alphanumeric passphrase).

Rahman et al and Brainard are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention it would have

been obvious to a person of ordinary skill in the art to combine the teaching of Rahman et al with modified Brainard method to design a method wherein credentials providing stronger encryption than the pass-phrase in order to provide transferring of a strong credential.

Regarding claim 4, Rahman et al discloses the credentials providing greater than 100 bits ofencryption (Col 3, starts at line 4; Col 7, starts at line 50; using strong password).

Regarding claim 5, Hypponen discloses the pass-phase having human-readable alpha-numeric characteristics. (Col 1, lines 40-65; passphrases)

12. Claim 18 and 20-26 are rejected under 35 USC 103 (a) as being unpatentable over Hypponen (US 6986050 B2) in view of Brainard (SecurSight: An Architecture for Secure Information) further in view of Bathrick et al (US 5825300).

Regarding claim 18, Hypponen discloses a method to facilitate a security connection between entities, comprising:

generating a strong password via a random generation function associated with a standard platform (Col 2, line 51 – Col 3,, line 30; generating long passwords);

generating a human readable pass-phrase (Col 2, line 51 – Col 3,, line 30; generating human readable long passphrase or password);

deriving a wrapping key from the pass-phrase (Col 3, lines 35-65; generating cryptographic key from passphrase)

Hypponen fails to disclose

wrapping the password cryptographically via the pass-phrase, wherein the wrapping key facilitates in encapsulating the password in a wrapper;

storing the wrapped password in an executable; and transmitting the executable and the pass-phrase to a system separately via different communications mediums.

However, Brainard discloses wrapping the password cryptographically, and wherein the wrapping key facilitates in encapsulating the password in a wrapper (Page 4 and 6, section 2.2, 2.3 and 3.5; an encrypted/ wrapped/ locked PSD or PAC that encapsulates authentication credentials such as keys or password; using a cryptographic key to wrap or lock the credentials/ PSD/ PAC); and storing the wrapped password in an executable (Pages 3-5; storage of PSD and PAC as executable codes, and cookies);

Modified Brainard - Hypponen system fails to disclose transmitting the executable and the pass-phrase to a system via different communications mediums.

However, Bathrick et al discloses transmitting the executable and the pass-phrase to a system via different communications mediums (Col 2, lines 33-40, 64-67; Claim 1; distributing keying material, and certificate material separately).

Brainard, Bathrick et al and Hypponen are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Bathrick et al with modified Brainard - Hypponen system to provide further protection against unauthorized access to the passphrase and the credential.

Regarding claim 20, Brainard discloses employing the key to unlock the strong password stored in the executable, the strong password employed to establish a trust relationship with an entity (Page 4 and 6, section 2.2, 2.3 and 3.5; unlocking the encrypted/ wrapped/ locked PSD or PAC with a cryptographic key). Furthermore, Hypponen discloses deriving a cryptographic key from a passphrase (Col 3, lines 35-65; generating cryptographic key from passphrase)

Regarding claims 21- 22, Brainard teaches a method comprising **at least one of:** Verifying an SSL certificate (Section 3.3" Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[Brainard teaches an application access agent and a certificate validation service to validate SSL certificates];

requesting a Universal Resource Locator (URL) from a listener(Section 2.4: Comparison with other authenticators)[Brainard teaches obtaining web browser based credentials which essentially refers to use of an URL] ; Presenting authentication credentials to a receiver (Section 3.3" Use of PACs by connect agent; Section 4.2: Certificate Validation Service) [.Brainard teaches desktop , presenting a certificate to be validated by the certificate validation service.];

logging in a caller to an account (Section 3.1: PAC definition; Section 3.3' use of: PACs by connect agents) [Brainard teaches a connect agent that initiates a client's access to an account after certificates are validated].

Regarding claim 24, Brainard teaches the method comprising **at least one of:** setting up account privileges; designating account contacts; and verifying contacts (Page 7, Col 1, Table 2, EAR; access right).

Regarding claim 25, Bathrick et al discloses a method comprising verbally communicating the password (Claim 3; non electronic communication medium for keying material/password).

Regarding claims 23 and 26, these limitations are already addressed in terms of rejecting claims 18, 22-23 and 25. Therefore, claims 23 and 26 are rejected applying as above rejecting claims 18, 22-23 and 25.

Conclusion

13. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system,

see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Abedin

Examiner, AU 2136

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136